CLAIMS

1. A processor-based device that prevents unauthorized use, comprising:

a processor for executing software instructions;

software instructions defining at least one user application;

a wireless communication subsystem that is operable to transmit and receive data utilizing a wireless protocol; and

software instructions defining a security protocol process that is operable to prevent execution of said software instructions defining said at least one user application by said processor when a message is received via said wireless communication subsystem, wherein said message indicates that said processor-based device is not in possession of a rightful user.

2. The processor-based device of claim 1 further comprising:

non-volatile memory, wherein said security protocol process is operable to store information in said non-volatile memory to indicate that execution of said software instructions defining at least one user application is not permitted.

3. The processor-based device of claim 2 wherein said non-volatile memory is flash memory.

4. The processor-based device of claim 1 further comprising:

user data, wherein said security protocol process is operable to prevent access to said user data when said message is received.

5. The processor-based device of claim 1 wherein said security protocol process is operable to cause said at least one user application to exit if said at least one user application is executing when said message is received.

6. The processor-based device of claim 1 further comprising:

a display, wherein said security protocol process causes said display to present information indicating that said rightful user is not in possession of said processor-based device.

7. The processor-based device of claim 1 wherein said security protocol process is implemented in an operating system of the processor-based device.

8. The processor-based device of claim 1 further comprising:

a basic input/output system (BIOS) that is operable to boot said processor-based device and is further operable to verify integrity of said security protocol process before completing boot operations.

9. A method for protecting a processor-based device from unauthorized use, wherein said processor-based device performs wireless communication, said method comprising:

receiving notice that said processor-based device is not in possession of a right user;

sending a message to said processor-based device to initiate a security protocol via a wireless communication protocol;

receiving said message by said processor-based device; and

initiating said security protocol on said processor-based device in response to said received message, wherein said initiating comprises preventing execution by said processor-based device of at least one user application that is defined by software instructions stored on said processor-based device in response to receiving said message by said processor-based device.

10. The method of claim 9 further comprising:

writing information in non-volatile memory of said processor-based device that said processor-based device is not in possession of said rightful user in response to said received message.

11. The method of claim 10 wherein said non-volatile memory is flash memory.

12. The method of claim 9 further comprising:

preventing access to rightful user data stored on said processor-based device in response to said received message.

13. The method of claim 9 further comprising:

displaying a message on a display of said processor-based device to indicate that said processor-based device is not in possession of said rightful user.

14. The method of claim 9 further comprising:

causing at least one user application to exit if said at least one user application is executing when said message is received by said processor-based device.

15. The method of claim 9 further comprising:

verifying integrity of executable code that implements said security protocol.

16. A system that prevents unauthorized use, comprising:

means for processing software instructions;

means for defining at least one user application;

means for transmitting and receiving data utilizing a wireless communication protocol; and

means for preventing execution of said software instructions defining said at least one user application by said means for processing when a message is received via said means for transmitting and receiving, wherein said message indicates that said system is not in possession of a rightful user.

17. The system of claim 16 further comprising:

means for preventing access to user data that is operable when said message is received.

18. The system of claim 16 further comprising:

means for storing information in non-volatile memory to indicate that said system is not in possession of said rightful user.

19. The system of claim 16 further comprising:

means for displaying information to indicate that said rightful user is not in possession of said system.

20. The system of claim 16 wherein said means for preventing execution is implemented in an operating system of said system.